Volume 51 | Issue 4 Article 9

2006

Privacy and Information Sharing in the War on Terrorism

Peter P. Swire

PRIVACY AND INFORMATION SHARING IN THE WAR ON TERRORISM

PETER P. SWIRE*

I. INTRODUCTION

SINCE the attacks of September 11, 2001, many voices have supported much greater information sharing to protect national security. The bipartisan *9/11 Commission Report* emphasized this point repeatedly.[1] For instance, the Report criticized the lack of information sharing between law enforcement and intelligence agencies,[2] between immigration databases and the Federal Bureau of Investigation (FBI),[3] among first responders[4] and between domestic and international collections of information.[5] The Report called for a major shift in philosophy, from the old "need to know" approach to a new culture of "need to share."[6] As discussed in this Article, the need for greater information sharing has been emphasized by President Bush, the Congress and expert groups such as the Markle Foundation Task Force on National Security in the Information Age.[7]

This Article accepts the need to share information in a wide variety of settings. It then asks the next questions—which information should be shared, with whom and under what circumstances? The central project of this Article is to create a due diligence list for proposed information sharing projects. For instance, will the information sharing program result in sharing secrets with our adversaries? Are there novel aspects of the pro-

* C. William O'Neill Professor of Law, Moritz College of Law of the Ohio State University. I am honored to include this Article in the Villanova Law Review Symposium in memory of privacy scholar Richard Turkington. Thanks to Bryan Cunningham and Kim Taipale for comments on an earlier draft. Thanks, as well, for the comments I received on this project in response to earlier versions of the current paper, at the University of Minnesota Law School, the University of Edinburgh Law School, the Oxford Conference on Safety and Security in a Networked World, the Annual Conference of Data Protection and Privacy Commissioners, the Battelle Policy Day Conference at the John Glenn Institute, the International Association of Privacy Professionals Annual Conference and the Villanova Law Review Symposium. My thanks to Meg Betzel for once again providing excellent research support.

1. *See generally* THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (official govt. ed. 2004).

2. *See id.* at 78-80.

3. *See id.* at 80.

4. *See id.* at 321.

5. *See id.* at 328.

6. *See id.* at 417.

7. For further discussion of the evolution of the current information sharing environment, see *infra* notes 8-13 and accompanying text.

posed system that may have unintended consequences? Are there ways that the proposed system may actually undermine security?

Part I of the Article describes the support for increased information sharing that has occurred in the wake of the attacks of September 11, 2001. The Article then examines the "Information Sharing Paradigm," which depends on three key premises: (i) the threat has changed; (ii) the threat is significant, especially due to weapons of mass destruction; and (iii) progress in information technology offers the most effective response to the new threat. Taken together, these three premises support greatly expanded information sharing to fight terrorism. Observers may vary in the degree to which they believe that the three premises are empirically true. Examination of the three premises, however, offers a helpful summary of the context for recent policy debates about information sharing.

Part II of the Article offers a "due diligence checklist" for assessing proposed programs of information sharing. Table 1 summarizes the checklist.

TABLE 1: DUE DILIGENCE CHECKLIST FOR A PROPOSED INFORMATION SHARING PROGRAM

1. Will the proposed sharing tip off adversaries?
2. Does the proposal improve security? Cost-effectively?
3. Is the proposal "security theater"? How much does it provide only the appearance of security?
4. Are there novel aspects to the proposed surveillance and sharing? What risks, if any, accompany these novel aspects?
5. Are there relevant lessons from historical instances of abuse? What checks and balances would mitigate risks of such abuse?
6. Do fairness and anti-discrimination concerns reduce the desirability of the proposed program?
7. Are there ways that the proposed measure could make the security problems worse?
8. What are the ramifications internationally and with other stakeholders?
9. Are there additional, privacy-based harms from the proposed measure?
10. Will bad publicity undermine the program?

This due diligence checklist highlights concerns about security, privacy and protection of civil liberties. There is a great urgency to adopt effective measures to fight terrorism and protect national security. In light of the urgency to take action, proponents of a new program can err on the side of optimism. They can conclude too readily that the program will improve security and have negligible side effects. In response, the due

diligence checklist can provide important rigor in analyzing new proposals. There are characteristic ways that information sharing programs might go wrong. We should check for those problems before implementing such programs.

II. RECENT SUPPORT FOR MUCH GREATER INFORMATION SHARING

This part of the Article summarizes the support for an enhanced "information sharing environment" to fight terrorism. By describing the "Information Sharing Paradigm," we can understand the essential logic that underlies information sharing proposals.

A. *The Information Sharing Environment*

The Introduction, above, summarized the concerns of the influential 9/11 Commission, which called for greatly enhanced information sharing in many settings.[8] The Bush administration has embraced the need for much greater information sharing. President Bush has issued at least half a dozen executive orders on the subject.[9]

Congress has agreed. At the end of 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004, which notably created the position of Director of National Intelligence in order to improve information sharing among the diverse intelligence agencies.[10] Section 1016 of the law, entitled "Information Sharing," calls for the creation of an "information sharing environment" and mandates staffing and guidelines for increasing information sharing for anti-terrorist purposes.[11]

---

8. For a further discussion of the concerns of the 9/11 Commission, see *supra* notes 1-6.

9. *See, e.g.*, Further Strengthening the Sharing of Terrorism Information to Protect Americans, Exec. Order No. 13,388, 70 Fed. Reg. 62,023 (Oct. 25, 2005) (updating information-sharing directives in light of Intelligence Reform and Terrorism Prevention Act of 2004); Continuance of Certain Federal Advisory Committees and Amendments to and Revocation of Other Executive Orders, Exec. Order No. 13,385, 70 Fed. Reg. 57,989, 57,989-90 (Sept. 29, 2005) (updating authorities of National Infrastructure Advisory Council); Strengthening the Sharing of Terrorism Information to Protect Americans, Exec. Order No. 13,356, 69 Fed. Reg. 53,599, 53,599 (Aug. 27, 2004) (directing agencies to give high priority to sharing of terrorism information); National Counterterrorism Center, Exec. Order No. 13,354, 69 Fed. Reg. 53,589 (Aug. 27, 2004) (creating National Counterterrorism Center to integrate information from multiple intelligence sources); Strengthened Management of the Intelligence Community, Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004) (calling for improved procedures for information sharing among intelligence community); Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security, Exec. Order No. 13,286, 68 Fed. Reg. 10,619, 10,621-22 (Feb. 28, 2003) (directing National Infrastructure Advisory Council to provide guidance to Secretary of Homeland Security on how to foster information sharing).

10. *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1011, 118 Stat. 3638 (2004).

11. *See id.* § 1016.

The Markle Foundation Task Force on National Security in the Information Age has been a key intellectual and policy supporter of greater information sharing. The Task Force has included a diverse set of former government officials, national security experts, technology experts and representatives of public interest groups. The Task Force issued major reports in 2002 and 2003.[12] These reports contain perhaps the most detailed and rigorous explanation of the need for greater information sharing, and how to do so consistent with other important values, such as privacy and civil liberties. Based on what I learned during my own participation in the latter stages of the Task Force's work, these reports were a significant factor in promoting the "information sharing environment" contained in the intelligence reform legislation of 2004.[13]

B. *The Information Sharing Paradigm*

In order to assess this shift toward information sharing, it is helpful to be explicit about its intellectual rationale. Commentators have widely discussed the "Bush Doctrine" for fighting terrorism, which prominently includes acting preemptively before an attack rather than responding after an attack occurs. The Bush administration justified the war in Iraq, for instance, under this doctrine of preemption.[14] The doctrine of military preemption has been accompanied by a shift toward prevention in the activities of law enforcement agencies, as shown in a 2002 report by the

12. *See* MARKLE FOUND., SECOND REPORT OF THE MARKLE FOUNDATION TASK FORCE, CREATING A TRUSTED INFORMATION NETWORK FOR HOMELAND SECURITY (2003), http://www.markle.org/downloadable_assets/nstf_report2_full_report.pdf; MARKLE FOUND., A REPORT OF THE MARKLE FOUNDATION TASK FORCE, PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE (2002), http://www.markle.org/downloadable_assets/nstf_full.pdf.

13. I became an "Associate" to the Markle Task Force early in 2005, and with Jeff Jonas, have been the lead author for MARKLE FOUND., IMPLEMENTING A TRUSTED INFORMATION SHARING ENVIRONMENT: USING IMMUTABLE AUDIT LOGS TO INCREASE SECURITY, TRUST, AND ACCOUNTABILITY (Feb. 2006), http://www.markle.org/downloadable_assets/nstf_IAL_020906.pdf. The views in the current Article, on privacy and information sharing, are clearly mine and not those of the Task Force. My writing here complements the work of the Task Force, and offers an intellectual framework for assessing whether and in what circumstances information sharing has net benefits.

14. The Administration's doctrine of preemption was set forth in THE PRESIDENT OF THE UNITED STATES, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 6 (2002), http://www.whitehouse.gov/nsc/nss.pdf, and was updated in THE PRESIDENT OF THE UNITED STATES, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 23 (2006), http://www.whitehouse.gov/nsc/nss/2006/nss2006.pdf ("The place of preemption in our national security strategy remains the same."). For one critique of the doctrine of preemption, see MARY ELLEN O'CONNELL, AM. SOC'Y OF INT'L LAW TASK FORCE ON TERRORISM. THE MYTH OF PREEMPTIVE SELF DEFENSE (2002), http://www.asil.org/taskforce/oconnell.pdf (criticizing preemptive self-defense doctrine as violation of international law).

Department of Justice: *Shifting From Prosecution to Prevention, Redesigning the Justice Department to Prevent Future Acts of Terrorism.*[15]

In this Article, I describe the rationale for what I call the "Information Sharing Paradigm." Later in the Article, I suggest possible critiques of this paradigm, but there is an appealing logic to the approach that should be understood even by those inclined to critique it. In order to preempt and prevent harm, greater information sharing is justified based on three propositions: the threat has changed; the threat is significant; and progress in information technology offers the most effective response to the new threat.

Proposition One is: the threat has changed. During the Cold War the biggest national security threats were a missile attack from the Soviet Union or a tank attack across Central Europe. These threats were large-scale and "symmetric," in the sense that the threat to the U.S. came from another nation state, using nuclear and conventional weapons that the U.S. also deployed. Today, by contrast, the threat is asymmetric. The risks come from a few individuals armed with box cutters (such as the 9/11 hijackers) or homemade explosives.

Proposition Two is: the threat is significant. Weapons of mass destruction (WMDs) are the central concern.[16] If the only risk were of occasional and small-scale attacks, harming up to a few dozen people at a time, then drastic new surveillance and other measures would likely not be justified. Preventing even a single nuclear attack, however, would be worth an enormous effort.

Proposition Three is: progress in information technology offers the most effective response to the new threat. Suppose you were an official in the Department of Homeland Security trying to decide on the mix of new physical security measures and information technology measures. You would be aware that the price of sensors, computer storage and information sharing networks has dropped sharply in recent years. You would know that the private sector is developing many new techniques for collecting and processing data and making decisions based on that data. Consequently, you would likely conclude that the efficient mix of security measures would have a large and ongoing shift toward information-intensive strategies.

---

15. U.S. DEP'T OF JUSTICE, FACT SHEET: SHIFTING FROM PROSECUTION TO PREVENTION, REDESIGNING THE JUSTICE DEPARTMENT TO PREVENT FUTURE ACTS OF TERRORISM (2002), *available at* http://www.fas.org/irp/news/2002/05/fbireorganizationfactsheet.pdf.

16. *See Transcript: Rumsfeld Cites Nexus of Terror and Weapons of Mass Destruction*, FED'N OF AM. SCIENTISTS NEWS (Feb. 4, 2002), http://www.fas.org/news/usa/2002/020402dod.html ("Secretary of Defense Donald Rumsfeld said that potential acquisition of weapons of mass destruction by terrorist groups constitutes the chief security threat facing the United States and the world today."). Judge Richard Posner recently defended much greater surveillance within the United States, based principally on the risks from weapons of mass destruction. *See* Richard A. Posner, *Wire Trap*, THE NEW REP., Feb. 6, 2006, at 15-16.

In short, the Information Sharing Paradigm rests on three simple propositions: the threat has changed; the threat is significant; and progress in information technology offers the most effective response to the new threat. I believe there is a powerful logic to the three propositions, and potential critics of information sharing should ponder the three propositions before opposing new initiatives.

C. *Assessing the Information Sharing Paradigm*

A full assessment of the three propositions is beyond the scope of this Article (or this author's expertise). To the extent all three propositions are valid, the case for information sharing is strengthened. To the extent any of them is less valid, then the urgency of information sharing will tend to be less.

1. *Proposition One: The Threat Has Changed*

I believe there is a strong case for Proposition One, that the threat has changed. The greatest Cold War threats to the United States were from large nation-states such as the Soviet Union, its Warsaw Pact allies and the People's Republic of China. The U.S. armed forces were deployed in West Germany, where "we faced the threat of Warsaw Pact forces charging through the Fulda Gap and driving for the English Channel."[17] The other greatest threat was that of nuclear attack, with the Soviet Union deploying a large number of inter-continental ballistic missiles.

The United States developed sophisticated intelligence tailored to the Cold War threats. Notably, the United States deployed aerial reconnaissance, first by high-altitude U2 airplanes and later by satellites.[18] This aerial reconnaissance worked relatively well against large and fixed targets, such as military bases in Eastern Europe and missile sites within the Soviet Union. The United States also developed human and signals intelligence that was targeted at agents of the Soviet Union and other foreign powers. The Central Intelligence Agency and National Security Agency took the lead on gathering intelligence abroad. Collection of foreign intelligence surveillance within the United States was eventually codified in the Foreign Intelligence Surveillance Act.[19]

---

17. *See* William J. Perry, *Message of the Secretary of Defense: The Dangers of the Post-Cold War World*, 1996 ANN. DEF. REP., *available at* http://www.defenselink.mil/execsec/adr96/message.html.

18. *See* Leonard David, Secret Cold War Spy Satellite Program Declassified by U.S. (Sept. 15, 2005), http://www.space.com/news/050915_nro_spysat.html (stating that U.S. satellites gathered electronic intelligence from Soviet naval ships from 1962-71); U2 Spy Plane, http://www.bergen.org/AAST/Projects/ColdWar/Arms/u2.html (last visited May 10, 2006) (explaining that United States responded to Soviet display of bomber planes by designing U2 spy plane).

19. For a history of foreign intelligence surveillance within the United States, see Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004).

One important feature of the Cold War was that enemy mobilization was often graduated and visible. There were occasional periods of high alert, such as during the Cuban missile crisis and several crises in the Middle East. Most of the time, however, the Soviet military was not on a state of high alert. In retrospect, the graduated and visible nature of enemy mobilization is a positive feature that seems lost to us today.

Today, by contrast, the major threats are asymmetrical. U.S. military spending roughly equals that of the rest of the world combined,[20] and there appears to be little reason to believe that any other country will soon challenge the United States militarily with conventional weapons.

In a period of asymmetrical threats, attacks are far less likely to occur after a graduated and visible mobilization. For those charged with homeland security, each day may be the day before the big attack. This perspective lends a sense of urgency to any measure that can reduce the risk of that attack—action must be taken immediately, or else it may be too late. In particular, those charged with homeland security have a strong desire to get information immediately, to help prevent the attack that might come at any moment. This desire to get information translates directly into the greater prominence of information sharing as a policy goal.

2. *Proposition Two: The Threat Is Significant*

Consider, for a moment, the possibility that the United States faces asymmetric threats but only of a low magnitude. Under this scenario, widespread new surveillance and information sharing programs would not be justified.

Public debates since 9/11, however, have generally assumed that "everything has changed" since the attacks of 2001. President Bush, in his address to Congress nine days after the attacks, called for expanded surveillance powers and said: "Americans have known surprise attack—but never before on thousands of civilians. All of this was brought upon us in a single day—and night fell on a different world, a world where freedom itself is under attack."[21]

It is beyond the scope of this Article to do an assessment of the actual risk from each type of possible nuclear, chemical, biological or other attack. I have written elsewhere about reasons to doubt that "everything has changed" after 9/11 or that the United States today faces greater threats

20. *See* Center for Arms Control and Non-Proliferation, U.S. Military Spending vs. the World, http://www.armscontrolcenter.org/archives/002244.php (last visited May 10, 2006) (showing that United States spent $522 billion in 2005, while rest of world spent $561 billion combined for same time period).

21. President George W. Bush, Address to a Joint Session of Congress and the American People (Sept. 20, 2001), http://www.whitehouse.gov/news/releases/2001/09/20010920-8.html.

than in other periods.[22] Greater research over time may show that anthrax and some other WMD attacks are considerably harder to stage than many have assumed.[23] With that said, the widely-held view thus far in the United States is that WMDs do pose very substantial threats, and the analysis of information sharing programs proceeds on that assumption. If, over time, the threat from WMDs appears lower, then there would be less justification for new information collection and sharing programs.

3. *Proposition Three: Progress in Information Technology Offers the Most Effective Response to the New Threat*

Beyond doubt, the U.S. intelligence agencies and the rest of the U.S. government should upgrade their information technology infrastructure. Information technology continues to evolve rapidly, and there is no excuse for using old and outdated computer systems and networks. Just as the private sector continually updates its information technology (IT) systems, so should the public sector.

As the price of information technology falls, and its performance increases, it also makes sense to shift from physical-based security to information-based security in a variety of settings. To take a simple example, the cost of human guards to patrol the perimeter of a facility stays roughly constant over time. Meanwhile, the cost has been going down sharply for surveillance cameras and the network to link those cameras back to a control room. As the relative cost of information-based defense declines, using information-based solutions more often is rational.

An additional reason for the United States to rely on information technology is to maintain and develop a comparative advantage in that sector. It will be relatively difficult for adversaries to develop counter-measures for advanced information technology. Research and development for homeland security and national security may produce commercial spin-offs, and intensive use of information technology will help ensure that the U.S. does not become vulnerable to information warfare attacks.

These reasons support a large and continuing investment in information technology for homeland and national security. They do not indicate, however, precisely *which* information collection and sharing measures are desirable. The next section of this Article creates a "due diligence" list for assessing those questions.

---

22. *See* Swire, *supra* note 19, at 1342-50 (presenting counterarguments to notion that threats to United States since 9/11 justify increased authority for surveillance).

23. According to Harvard expert Dr. Richard Zane: "How easy is it to spread anthrax? It is extremely difficult." Interview by Aetna InteliHealth with Dr. Richard Zane, Chairman of the Disaster Committee, Brigham and Women's Hospital (Oct. 10, 2001), http://www.intelihealth.com/IH/ihtIH/WSIHW000/333/24524/336414.html?d=dmtICNNews.

III. A DUE DILIGENCE CHECKLIST FOR INFORMATION SHARING PROPOSALS

This part of the Article sets forth ten due diligence questions for assessing proposed information sharing programs. The emphasis in these questions is on the downsides of information sharing; proponents of a program will often be optimistic about what it can achieve, and the due diligence process (in corporate takeovers or for information sharing) is designed to highlight possible problems that may need to be addressed.

A. *No Presumption of Information Sharing Where It May Tip Off an Adversary*

In deciding whether to share information with allies (everyone who is considered friendly), a key question is the extent to which that action may also share information with adversaries. To take a simple example, consider the question of how broadly to share the names of individuals who are on a watch list. Greater information sharing clearly helps to the extent that many border guards and other allies may use the list to catch the suspects. On the other hand, sharing information with many border guards increases the possibility that suspects will be tipped off that they are on the list, and thereby elude capture.

The first step in due diligence, then, is to analyze the incremental benefit of information sharing with allies compared with the incremental risk that the sharing will benefit one's adversaries. This Article will briefly describe recent research on that topic, and then apply the research to the topic of information sharing for intelligence purposes in the war against terrorism.

1. *The Security Disclosure Model*

Much of my recent research has analyzed the implications of what I call the "Security Disclosure Model," which addresses the topic of when disclosure helps or hurts security.[24] The model has direct implications for information sharing, which is disclosure that is designed to go only to one's allies.

The Security Disclosure Model begins with a paradox. Most experts in computer and network security are familiar with the slogan, "there is no

24. The basic approach is set forth in Peter P. Swire, *A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?*, 3 J. ON TELECOMM. & HIGH TECH. L. 163 (2004) [hereinafter Swire, *Security Model*], *available at* http://ssrn.com/abstract=531782. A slightly updated version of the material was published as Peter P. Swire, *A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?*, *reprinted in* THE LAW AND ECONOMICS OF CYBERSECURITY 29 (Mark F. Grady & Francesco Parisi eds., 2005). A second article analyzed the incentives facing key actors making the decision of whether to disclose. *See* Peter P. Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems*, 42 HOUS. L. REV. 1333 (2006), *available at* http://ssrn.com/abstract=842228.

security through obscurity."[25] For proponents of Open Source software, revealing the details of the system will actually tend to improve security, notably due to peer review. On this view, trying to hide the details of the system will tend to harm security because attackers will learn about vulnerabilities, but defenders will not know where to patch the vulnerabilities. In sharp contrast, a famous World War II slogan warns, "loose lips sink ships."[26] Most experts in the military and intelligence areas believe that secrecy is a critical tool for maintaining security. The paradox is that both views—that disclosure helps security and hurts security—cannot simultaneously be correct. The task of the Security Disclosure Model is to explain the conditions for when each view, the Open Source view and the military view, is correct.

The first step toward resolving the paradox is to examine the effects of disclosures on attackers and defenders. Where disclosure on balance helps the attackers, then those defending the systems should rationally keep secrets. Where disclosure on balance helps the defenders, then disclosure should result.

By focusing on "effects on attackers" and "effects on defenders," the Security Disclosure Model highlights the conditions under which the Open Source and military views are each correct. For Open Source, the usual assumption is that disclosure will not help attackers much or at all. In a world of rapid communications among attackers where exploits are spread on the Internet, a vulnerability known to one attacker is rapidly learned by others. For Open Source, the next assumption is that disclosure of a flaw will prompt other programmers to improve the design of defenses. In addition, disclosure will prompt many third parties—all of those using the software or the system—to install patches or otherwise protect themselves against the newly announced vulnerability. In sum, disclosure does not help attackers much but is highly valuable to the defenders who create new code and install it.

In contrast, the military assumptions highlight the ways that disclosure can assist the attackers. For a military base, for instance, the precise location of machine guns and other defenses is a closely guarded secret. A major goal is to hide the defenses until it is too late for attackers, so that they fall into traps. In terms of disclosure helping defenders, the military traditionally uses its chain of command to tell fellow defenders what they need to know. There is no general broadcast of security flaws because such a broadcast would help the attackers but provide little or no information to fellow defenders.

That brings us to the topic of the current Article, the intermediate case that the Security Disclosure Model calls "information sharing." The Model treats information sharing as indeterminate—there is no presumption either in favor of or against information sharing. To the extent the

25. *See* Swire, *Security Model*, *supra* note 24, at 165 n.2.

26. *See id.* at 165 n.4.

information is shared with allies—the "good guys"—then there can be strong assistance to the defenders because they might catch the terrorists before the attack occurs. To the extent the information is shared with adversaries—the "bad guys"—then information sharing can be the tip-off that lets the attackers escape or change their plans. This dual effect of information sharing—to help defenders *and* attackers—is a helpful way to understand why information sharing has been so important and yet so difficult a topic since the attacks of September 11, 2001.

Briefly, a fourth possibility under the Model is where additional disclosure about a vulnerability will have only small effects on attackers and defenders. This possibility is called the public domain.

Table 2 pulls the four scenarios together. Notably, the Open Source scenario shows reasons for openness, with disclosure having a large help-the-defenders effect and a low help-the-attackers effect. The military scenario shows the opposite, with disclosure harming the defenders and helping the attackers. For information sharing, disclosure helps both attackers and defenders, making it unclear when to disclose. For the public domain, additional disclosure has minor effects.

TABLE 2

	HELP-THE-ATTACKERS EFFECT		
HELP-THE-DEFENDERS EFFECT		*Low*	*High*
	High	Open Source	Information Sharing
	Low	Public Domain	Military/Intelligence
Greater Disclosure Up and to the Left Greater Secrecy Down and to the Right			

2. *Applying the Security Disclosure Model*

My previous writing goes into considerable detail about when disclosure is most and least likely to aid security. A few highlights are important to the discussion of information sharing.

Some categories of activity have especially strong reasons for secrecy. First, even the strongest Open Source advocates understand the importance of keeping passwords and cryptographic keys secret. Handing out these secrets directly helps attackers but does not assist defenders. Sharing of passwords and keys should occur only on a need-to-know basis.

Second, there is a compelling logic to the longstanding principle of keeping sources and methods secret. It will often be difficult for attackers to learn about the sources and methods except from the defenders. Proponents of information sharing should thus be cautious about sharing the name of a source, such as the identity of an intelligence agent, or sharing methods that enemies have difficulty detecting, such as a new form of surveillance that provides useful information.

Third, and more generally, there are strong reasons for secrecy about surveillance activities. By their nature, surveillance activities are difficult for outsiders to detect. The outsiders thus do not typically learn much about surveillance over time. Widespread information sharing about surveillance activities thus can undermine security, because sharing increases the likelihood that surveillance targets will adopt counter-measures. With that said, however, the security advantages of secrecy about surveillance should always be accompanied by assessment of the many other reasons for oversight and other accountability in connection with surveillance, in order to uphold crucial values including privacy, free speech and civil liberties.

By contrast, there are sometimes scenarios where disclosure directly assists security. One scenario involves deterrence, where disclosure about the defense is intended to discourage attacks. Another scenario is where attackers already know about a vulnerability, but action is needed by defenders to increase protection. For instance, terrorists may know about vulnerabilities in a city's water supply or other infrastructure. In such circumstances, there is likely to be a benefit from information sharing, because the city may defend itself better but the attackers learn nothing new.

Along with these categories that tend to support secrecy or disclosure, there is a pervasive question of how well "selective disclosure" will succeed. In an ideal world, information could be shared with a large number of "good guys" but there would be no leaks to the "bad guys." In practice, leaks are more likely the more people who know a secret. For example, consider the risk of a leak as information goes from compartmentalized within one federal agency, to available throughout the agency, to available across multiple federal agencies, to available to cleared individuals in states and localities, to available to all first responders.

One response to the risk of leaks is to perform more, and more thorough, background checks. This strategy is likely to make sense for information that is accessed by only a select few. It is difficult to imagine, however, that any background check process will succeed in keeping information secret if the secret goes to all first responders in the United States. The likelihood is simply too great that there will be one "bad guy" who gets through the background check, or who is compromised after completion of the background check.

Relying on selective disclosure and background checks faces another problem beyond the sheer number of people who know a secret. In some

situations, the most knowledgeable people are those with the closest relationship to a region or situation. Their local knowledge makes them uniquely useful but also uniquely risky from the perspective of a background check. For instance, consider an immigrant and native speaker from a region that is now in conflict. The language skills and cultural insights may be essential to understanding a wiretap or other intelligence. Yet the immigrant may have family or friends aligned with opposition groups, making it difficult to complete a clean background check.

To summarize the implications of the Security Disclosure Model, it is vitally important to assess the likely benefits of sharing with allies compared with the risks that the information will be shared with adversaries. The Model highlights situations where the net benefits of sharing are likely to be especially high or low, but a judgment about the net benefits depends in practice on empirical assessment of a number of factors. As the Markle reports indicate, there are many risks that come from *not* sharing information. At a fundamental level, however, due diligence is needed. There should be no presumption of sharing or not sharing data.

B. *Ends/Means Rationality: Does the Proposed Measure Improve Security? Cost-Effectively?*

The Security Disclosure Model focuses on the possibility that information sharing will help adversaries. The other most general part of due diligence is to assess the extent to which the proposed measure actually does what it is supposed to do. Are the means (the proposed program) likely to achieve the ends (increasing security)? Does the proposed program increase security in a cost-effective way, in light of the other ways we might spend our resources?

The obvious methodology for this task is to apply cost/benefit analysis ("CBA") to proposed information sharing programs. For the past three decades, both Republican and Democratic administrations have applied a CBA to major regulations, including proposed environmental and safety measures.[27] The basic idea is that scarce resources in the public and private sectors should only be spent in areas where there are likely to be net benefits to society. As experience with CBA has grown, the process has specifically acknowledged the role for qualitative assessment in addition to purely quantitative estimates of risks and benefits.[28] The most important

27. Presidents Reagan and Clinton required administrative agencies to perform CBA on regulations. *See* Regulatory Planning and Review, Exec. Order No. 12,866, 58 Fed. Reg. 51,735 (Sept. 30, 1993) (mandating that agencies choose regulatory options that "maximize net benefits"); Exec. Order No. 12,291, 46 Fed. Reg. 13,193 (Feb. 17, 1981) (requiring CBA be performed on regulations). For one discussion of the history and theory, see Robert W. Hahn & Cass R. Sunstein, *A New Executive Order for Improving Federal Regulation? Deeper and Wide Cost-Benefit Analysis*, 150 U. PA. L. REV. 1489 (2002).

28. *See* Regulatory Planning and Review, Exec. Order 12,866, 58 Fed. Reg. 51,735, 51,735 (Sept. 30, 1993).

step, in my view, is to insist on a logical, qualitative statement of how the proposed program is intended to operate and why that is likely to lead to a desirable outcome.[29]

The topic of data mining can illustrate this sort of qualitative analysis. The credit card industry has a well-known and generally successful model of data mining. When a credit card is used for an "out of pattern" purchase, authorization for the charge may be declined or the cardholder may receive a phone call to confirm that the charge is made by the legitimate cardholder. This sort of data mining is widely credited with reducing credit card fraud.[30]

That does not mean, however, that all data mining will be similarly successful. The credit card system has several attributes that contribute to successful data mining: (1) a very large number of valid actions (non-fraudulent purchases); (2) a large number of bad actions (fraudulent purchases); (3) repeated types of attacks that have a pattern (thieves have common patterns of using a newly-stolen card); and (4) the low cost of false positives. "False positives" here refer to valid purchases for which the system issues an alert. The cost of false positives for credit cards is reasonably low in part because the valid cardholder receives a simple phone call to determine whether a purchase is valid. Even if a purchase is refused to the valid cardholder, that person may be able to purchase the item with a different card, may speak with the card company and provide proof of identity or at worst can often purchase the item once the problem is fixed.[31]

Data mining to stop terrorism is quite different than data mining in the credit card system. In contrast to having large numbers of fraudulent purchases every day, the number of terrorist attacks is extremely low. In contrast to having repeated purchasing patterns of credit card thieves, each terrorist attack may be first-of-a-kind (the first airplane attack into an office building, the first shoes set on fire, etc.). In addition, the cost of false positives is likely to be much higher, in at least two respects. First, the effect on someone falsely labeled a "terrorist" can be very high—imprisonment, failure to pass a background check and so on. Second, the cost to the government of checking out false positives can also be much higher

29. There are important and complex arguments about the desirability and possible limits on the usefulness of CBA. *See, e.g.*, Frank Ackerman & Liza Heinzerling, *Pricing the Priceless: Cost-Benefit Analysis of Environmental Protection*, 150 U. PA. L. REV. 1553 (2002). The position I advocate here, however, avoids the bulk of the criticisms, because the emphasis is on a logical, qualitative analysis instead of a process that emphasizes quantification of difficult-to-measure outcomes.

30. *See* Torsten Ove, *Thief May Get a Charge Out of This*, PITTSBURGH POST-GAZETTE (May 7, 2004), *available at* http://www.post-gazette.com/pg/04128/312606.stm (describing how one thief was caught while making "out of pattern" purchase).

31. Bruce Schneier has written a similar analysis of data mining for terrorism. Bruce Schneier, *Why Data Mining Won't Stop Terror*, WIRED (Mar. 9, 2006), http://www.wired.com/news/columns/0,70357-0.html.

than the simple phone call to the credit card customer. Each lead may require trained investigators to do a substantial investigation of a person who may be a dangerous terrorist. The investigation should be done in a way that does not cause the terrorist to flee.

The analysis here does not conclude that data mining is necessarily helpful or unhelpful in fighting terrorism.[32] Instead, the analysis is designed to be an example of qualitative cost/benefit analysis. In what circumstances will data mining most likely spot useful patterns? In what circumstances will the costs of false positives outweigh the benefits of identifying potential suspects? These sorts of inquiries will help ensure that proposed programs are effective, and cost-effective, in fighting terrorism.

C. *Is the Program "Security Theater"? How Much Does It Provide the Appearance of Security?*

A related way to test a proposal's usefulness is to use the colorful term coined by Bruce Schneier—"security theater." As Schneier says in his book *Beyond Fear*, "some countermeasures provide the feeling of security instead of the reality."[33] In more neutral language, the question is the extent to which a measure provides actual security versus the appearance of security.

To understand the concept, imagine that you are an advisor to the Secretary of Homeland Security. A meeting has been called to protect "X," where X can be any possible target of a terrorist attack, such as an office building, a major port or the southern border of the United States. The Secretary is going to testify before Congress shortly on the topic. Suppose that you have analyzed five proposed security measures, and decided that none of them is effective at preventing an attack and all are costly to implement. At the meeting, you are asked to recommend what to do. One possibility is that the Secretary could appear before Congress and say: "We have looked at all the options, and decided that there are no security measures that are cost-effective, so we are going to do nothing at all."

How will this approach play with Congress and the press? In my experience, not well at all. There is a great temptation to show that one is "doing something" and to describe concrete measures being taken in an area. In assessing a proposed information sharing or other security measure, it is thus useful to specifically analyze the extent to which a measure creates security or the appearance of security.

Although Schneier does not make the distinction explicit, there appears to be at least two components to security theater. The first is the

32. For an especially rigorous and well-researched defense of data mining for homeland security purposes, see K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2, 67-72 (2003).

33. BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD 38 (2003) (emphasis omitted).

possibility that the appearance of security is itself a reasonable goal. For instance, Schneier mentions that, in the wake of the 9/11 attacks, "the U.S. government posted armed National Guard troops at airport checkpoints . . . (but were smart enough not to give them bullets)."[34] It seems to me quite possible that such a measure was beneficial in establishing calm and promoting trust in air travel immediately after the attacks. In such instances, a moderate amount of theater may produce a moderate amount of good, in restoring calm and confidence.

A second component of security theater, however, is where a measure is implemented primarily due to bureaucratic or political pressures to "do something" about security. One example may be a security measure that spread among office buildings in U.S. cities after the 9/11 attacks. People who visited the office buildings were asked by a guard to show I.D. before entering. In my view, it is hard to see how this ritual improved security at all.[35] Anyone planning a significant attack would simply show an authentic (or fake) I.D. on his or her way into the building. Yet building managers seem to have wanted to show they were "doing something" to increase security.

In short, analysis of a proposed information sharing or other security proposal should consider the possibility that the proposal is security theater rather than a measure that will actually deter or respond to an attack. At the very least, this analytic step is important for security planners, to make sure that the defenders are not themselves fooled by theatrics into thinking effective security is in place if it is not.

D. *Identify the Novel Nature of Proposed Surveillance and Sharing*

A next part of due diligence is to consider the novel aspects of a proposed program and consider whether the innovation is justified. This conservative intuition is associated with the name of Edmund Burke, who criticized many innovations of the French Revolution for their radical nature and unintended consequences.[36] An eloquent summary of Burkean conservatism comes from supply-side economist Jude Wanniski: "[S]ociety is a vast and complicated historical product which may not be tinkered with at will like a machine; it is a repository of collective human wisdom to be regarded with reverence, and if reformed at all it must be with due respect for the continuity of its traditions."[37] In the words of philosopher and economist Friedrich Hayek, "the result of the experimentation of

34. *Id.*

35. Kim Taipale has suggested that additional layers of security, even when weak, may be useful because they raise the costs to terrorists of learning about the defenses and "provide additional points of potential error on the part of the terrorist that may lead to discovery." *See* Taipale, *supra* note 32, at n.285.

36. *See generally* EDMUND BURKE, REFLECTIONS ON THE REVOLUTION IN FRANCE (Anchor Books 1973) (1790).

37. *See* Jude Wanniski, *Edmund Burke's Conservatism*, POLYCONOMICS (June 19, 1998), http://www.polyconomics.com/searchbase/06-19-98.html.

many generations may embody more experience than any one man possesses."[38]

At a common-sense level, the Burkean point suggests the usefulness of considering possible advantages of the status quo and possible disadvantages of a new program. There may be good reasons that practices and institutions have historically developed in a certain way. There may be unintended consequences of a well-intentioned reform. Enthusiasm for the new proposal should be accompanied by thoughtfulness about whether things will work out as proponents imagine.

Two current examples suggest the usefulness of the Burkean point. The first example concerns the controversy about whether library records should be available to the government under Section 215 of the Patriot Act.[39] Proponents of government access do not wish to give terrorists a safe haven in libraries to communicate online. Opponents, on the other hand, stress how much government access to library records differs from historical practice, where stricter-than-usual rules have limited government access to the reading habits of individuals.[40] The Burkean point is that there may be good reasons why states historically have enacted special privacy laws for library records. Any proposed change should consider this special historical experience.[41]

A second example does not involve information sharing but instead a related debate in the fight against terrorism: whether the time has come for the United States to have a national I.D. card. The Real ID Act of 2005, with its requirement of national standards for drivers' licenses, is a significant step toward having such a card.[42] Without trying to debate all of the issues about a national I.D. system,[43] the Burkean point is a simple one. The longstanding tradition of avoiding a national I.D. card is itself a reason for caution in moving forward. There are quite possibly important reasons why use of the identity card has been eschewed in the many emer-

38. F. A. HAYEK, THE CONSTITUTION OF LIBERTY 62 (1960).

39. For a further discussion of Section 215 and library records, see Swire, *supra* note 19, at 1331-32, 1356-59. The provisions concerning searches of library records were somewhat modified in the 2006 reauthorization of the Patriot Act.

40. *See* Kathryn Martin, Note, *The USA Patriot Act's Application to Library Patron Records*, 29 J. LEGIS. 283, 295 (2003).

41. I have made a similar argument against the "gag rule" in Sections 215 and 505 of the Patriot Act. These rules prohibit individuals who have received certain orders to produce documents to disclose the fact of the search. One argument against the gag rules is how much they differ from historical practice for physical searches. *See* Swire, *supra* note 19, at 1359-60.

42. The Real ID Act was passed as Division B of an Act Making Emergency Supplemental Appropriations for Defense, the Global War on Terror, and Tsunami Relief, for the fiscal year ending September 30, 2005, and for Other Purposes, Pub. L. No. 109-13, 119 Stat. 231 (2005).

43. A recent report from the National Academy of Sciences examines the many technical and institutional obstacles to effective implementation of a national I.D. card. NAT'L ACAD. OF SCIS., COMPUTER SCI. AND TECH. BD., IDs—NOT THAT EASY: QUESTIONS ABOUT NATIONAL IDENTITY SYSTEMS (2002).

gencies that have faced the United States since its founding. Enthusiasm for possible advantages of an identity card should be tempered by consideration of why it has not been adopted previously.

How is one to apply the Burkean point in assessing a proposed security program? To begin with, the status quo should not be exalted as some ideal state. Burke himself wrote: "A state without the means of some change is without the means of its conservation."[44] The Burkean point instead is a useful corrective to the tendency to believe that "everything has changed" since 9/11.[45] Many things have changed since those attacks, but many things have not. As a step in the due diligence for proposed programs, it is useful to identify the novel aspects of a proposed program, consider possible unintended consequences, and then move forward if, and only if, the case for the new program is convincing.

E. *Consider Historical Abuses and Implement Checks and Balances*

The history of government surveillance is linked with a history of government abuse. The Framers of the United States Constitution reacted to the problem of general warrants with the Fourth Amendment, which begins by stating: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[46] By including "papers and effects," the text underscores the importance of protecting people's communications and records from unreasonable government searches. Such communications and records are often the subject of information sharing proposals. Even where changing practices mean that the Fourth Amendment does not literally apply,[47] the principle of preventing abuse of government power nonetheless remains important. Part of due diligence for assessing information sharing programs, therefore, is an assessment of historical patterns of abuse and the corresponding need to create checks and balances against such problems.

The policy of prevention carries with it particular risks of abuse. Since September 11, FBI Director Mueller has announced that prevention of terror attacks is the top priority of the agency.[48] In making prevention the priority, the Bureau is returning to the heavy emphasis on prevention

---

44. *See* BURKE, *supra* note 36, at 33.

45. I have elsewhere critiqued the view that "everything has changed" since September 11. *See* Swire, *supra* note 19, at 1342-48.

46. U.S. CONST. amend. IV.

47. For two excellent analyses of gaps in statutory and Fourth Amendment protections for online activity, see Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1380 (2004); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1582-96 (2004).

48. *See* David Johnson, *9/11 Congressional Report Faults F.B.I.-C.I.A. Lapses*, N.Y. TIMES, July 23, 2003, at A12.

adopted by Director J. Edgar Hoover in the fight against Communists and other "subversives."

A detailed history of FBI activities from the Hoover period comes from the 1976 "Church Committee" Report, named for Senator Frank Church.[49] According to this report, after World War II, "preventive intelligence about 'potential' espionage or sabotage involved investigations based on political affiliations and group membership and association. The relationship to law enforcement was often remote and speculative . . . ."[50] Until the Church Committee's hearings, the FBI continued to collect domestic intelligence under "sweeping authorizations" for investigations of "'subversives,' potential civil disturbances, and 'potential crimes.'"[51] Based on its study of the history, the Church Committee concluded:

> The tendency of intelligence activities to expand beyond their initial scope is a theme which runs through every aspect of our investigative findings. Intelligence collection programs naturally generate ever-increasing demands for new data. And once intelligence has been collected, there are strong pressures to use it against the target.[52]

In addition to this tendency of prevention to lead to expanding surveillance and information sharing, my previous writings have identified other concerns raised in earlier eras of expanded surveillance in the United States. These other concerns include: routine violations of law; secrecy; use against political opponents; targeting and disruption of unpopular groups; chilling of First Amendment rights; harm to individuals; distortion of data to influence government policy and public perceptions; and cost and ineffectiveness.[53]

What are we to make of these experiences as we consider new information sharing projects? One answer comes from a longtime civil servant who has participated in information sharing projects in recent years: "We

49. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, 94TH CONG., FINAL REPORT ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK II, § I (1976) (internal citations omitted) [hereinafter CHURCH FINAL REP. IIA], *available at* http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIa.htm.

50. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, 9TH CONG., FINAL REPORT ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK II, § II, U.S. Senate, Apr. 26, 1976 (footnotes omitted), *available at* http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIb.htm.

51. *Id.*

52. CHURCH FINAL REP. IIA, *supra* note 49.

53. *See* Swire, *supra* note 19, at 1315-20. Paul Rosenzweig, now an official in the Department of Homeland Security, has written a thoughtful article that emphasizes the greater checks against abuse that exist today than in previous periods. *See* Paul Rosenzweig, *Civil Liberties and the Response to Terrorism*, 42 DUQ. L. REV. 663, 671-74 (2004).

don't need a new law. We need a ninth grade history teacher."[54] Knowledge of history reduces the likelihood that we will repeat it. Until recent years, federal agency meetings often included veterans of the Church Committee era, and these veterans often had vivid personal memories of the problems the agencies faced when excessive surveillance was uncovered.[55] Today, however, many of those veterans have retired. Education in the history of abuses is thus one sensible step for those who are assessing new information sharing and other surveillance programs.

The due diligence, I believe, begins with knowledge of the history. The second step is to consider what checks and balances are in place against possible future abuse. I am not a pessimist who believes that intelligence activities inevitably will return to the level of problems seen in earlier periods. I do believe, however, that human nature has remained largely unchanged since then. Unless effective institutional safeguards exist, large and sustained expansions of domestic intelligence activity, in the name of national security, can quite possibly recreate the troublesome behaviors of the past.

F. *Do Fairness and Anti-Discrimination Concerns Reduce the Desirability of the Proposed Program?*

A next lens for examining a proposed information sharing program concerns racial and ethnic profiling. The due diligence here concerns the fairness and efficacy of such profiling.

The case for profiling was made in a particularly blunt way by Neil Livingstone, CEO of the international security firm GlobalOptions: "Young Islamic males, like it or not, are the enemy. There is no getting around it, we have to profile them."[56] Some leading criminal justice scholars have given at least qualified support to ethnic profiling.[57] Information collection and sharing projects thus may target "young Islamic males" or other groups that are thought to be especially likely to pose security risks.

In response, former prosecutor and now Ohio State law professor Sharon Davies has written a closely-reasoned and persuasive article on "Profiling Terror."[58] Professor Davies summarizes potential harmful effects of explicit racial targeting:

54. The civil servant who made this remark to me asked not to have it attributed to him.

55. During my own federal service in 1999 until early 2001, I heard such statements from veterans of the Church Committee era.

56. Wendy Ruderman, *Arab-Americans Upset by Profiling*, BERGEN REC., Sept. 23, 2001, at A1.

57. *See, e.g.*, Samuel R. Gross & Debra Livingston, *Racial Profiling Under Attack*, 102 COLUM. L. REV. 1413, 1437 (2002); William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2161 (2002).

58. *See generally* Sharon L. Davies, *Profiling Terror*, 1 OHIO ST. J. CRIM. L. 45 (2003). Davies's work builds on excellent earlier scholarship by David Harris. *See* David A. Harris, *The Stories, the Statistics, and the Law: Why "Driving While Black" Matters*, 84 MINN. L. REV. 265 (1999).

> It takes a profound emotional toll on those subject to it. It is degrading and intimidating. It also has serious group effects. It treats innocent, law-abiding people like criminals purely on the basis of race or ethnicity. It encourages [those targeted by profiling] to be mistrustful of and to avoid contact with the police, and heightens racial tensions when those contacts occur. It solidifies racial divides and racial prejudices, as Whites equate greater Black arrests with greater Black criminality. And it is fundamentally inconsistent with equality principles supposedly at the center of our political and social system.[59]

Due diligence on ethnic profiling would seem to include at least three components. First, ethnic profiling by government can be unfair and perceived as unfair. To what extent does a proposed program violate legal and ethical principles of equality, and can steps be taken to reduce inequality or mitigate its effects?

Second, Davies's article provides a series of reasons to doubt the empirical case for the usefulness of ethnic profiling. She states: "In a nation that claims upwards of 3.5 million persons of Arab ancestry, the ethnic characteristic of Arab descent, standing alone, possesses no useful predictive power for separating the September 11 terrorists' accomplices and other terrorist wannabees from innocent Americans."[60] Davies surveys the history of racial and ethnic profiling, including an empirical study that showed that black drivers were stopped more often while driving on an interstate highway in Maryland but actually had contraband at a lower rate than white drivers.[61] In terms of terrorism, Davies points out that the Oklahoma City and Unabomber attacks were done by white males from upstate New York, yet there have been no profiling proposals of that group.[62] Davies concludes: "In light of the human tendency to overestimate the value of racial and ethnic proof, a presumption against its consideration is appropriate."[63] Even if one does not agree with a strong presumption against profiling, the history of over-reliance on profiling is itself a good reason to proceed cautiously with new profiling proposals.

Third, ethnic profiling can undercut cooperation from the community that is targeted.[64] Suppose you were a member of a community that is

59. Davies, *supra* note 58, at 73-74 (citations omitted).

60. *Id.* at 52.

61. *See id.* at n.56 (collecting several similar study results).

62. *See id.* at 78-79 (documenting attacks of several American-born terrorists). I myself grew up in upstate New York, and would not welcome profiling on that basis.

63. *Id.* at 75.

64. *But see, e.g.*, EUROPEAN MONITORING CENTRE ON RACISM AND XENOPHOBIA, THE IMPACT OF 7 JULY 2005 LONDON BOMB ATTACKS ON MUSLIM COMMUNITIES IN THE EU 21-23 (2005), *available at* http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/10_11_05_attacks_report.pdf (discussing new measures taken by authorities after July 2005 bombing on London underground to try to increase cooperation with local Muslim community).

seen by some as a source of danger to other groups in society, such as black neighborhoods during the riots in the 1960s or Arab American communities today. For the police, an important question is whether profiling produces more information about crimes (by catching more possible criminals) or less information (by alienating the targeted community and drying up sources of leads). I am not aware of any general theory that determines when harsh measures, including those based on race and ethnicity, become counter-productive. To the extent cooperation with the government is needed to prevent crime and terrorist attacks, then it is important to consider the possibility that profiling measures will reduce that cooperation.

G. *Are There Ways the Proposed Measure Could Make Security Problems Worse?*

One useful part of due diligence is to consider the possibility that a proposed measure will actually make the problem worse. The discussion of ethnic profiling raised this possibility—perhaps harsher profiling of a community will reduce cooperation so that the authorities actually learn less than they would have without the profiling.

As a logical matter, the possibility of a measure undercutting itself is part of an earlier item on the due diligence list, whether the proposal is effective and cost-effective at promoting security. As a matter of performing due diligence, however, I suggest that the possibility of a measure undercutting itself is a useful tool of a devil's advocate. By focusing one's attention on the possibility of a self-defeating consequence, one is sometimes able to spot a problem that would otherwise have been overlooked.

One example has been raised by Bruce Schneier and earlier researchers in connection with proposed "trusted traveler" programs.[65] Such programs would do background checks of air passengers who volunteer for them. Passengers who pass the background check get access to faster lanes at airport security and are exempt from secondary screening. This sort of program could understandably be attractive to frequent flyers, who otherwise stand in the standard, longer security lines.

Schneier critiques the program in this way: "Imagine you're a terrorist plotter with half a dozen potential terrorists at your disposal. They all apply for a card, and three get one. Guess which three are going on the mission? And they'll buy round-trip tickets with credit cards, and have a

65. For one official document supporting a trusted traveler program, see Press Release, Office of the Press Sec'y, Dep't of Homeland Sec., United States, Mexico and Canada Deliver Initial Security and Prosperity Partnership Report (June 27, 2005), http://www.dhs.gov/dhspublic/display?content=4552. For important earlier research on how terrorists will adapt to a trusted traveler program, see Samidh Chakrabarti & Aaron Strauss, *Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System* (2002), *available at* http://www.swiss.ai.mit.edu/6805/student-papers/spring02-papers/caps.htm.

'normal' amount of luggage with them."[66] A program designed to enhance security can thus undermine security by creating a clear path to the airplane for the terrorists who pass the background check.

Another example comes from a visit I made to Europe in the fall of 2005, when the European Union was considering a data retention proposal, which was later adopted.[67] The program requires telephone companies and Internet service providers (ISPs) to retain records of phone calls, emails and web surfing for six months or more. At the time of the conference, there were contentious arguments about the proposal, focusing mostly on the privacy risks that come from storing all the communication records.

I was giving an earlier version of this Article at the conference, and so I applied the "does the proposal undermine security" question to the data retention plan. A new insight quickly emerged. The data retention proposal creates a risk to police forces and intelligence agencies whose own communications records now would be stored by telephone companies and ISPs.[68] Terrorists and criminals who could infiltrate the ISPs could now get insights into police and intelligence activities.[69] The proposed security measure of data retention thus created a new security vulnerability.

Note that discovery of such a vulnerability does not indicate what action to take. For some, discovery of the vulnerability might tilt the risk/benefit calculus, and lead to opposition to the data retention proposal. For others, the data retention measure may still seem worthwhile, but now measures should be considered to address the vulnerability. In either case, the devil's advocate analysis was useful. By asking the question of whether a security measure undermined security, certain risks of the program became apparent that had not previously surfaced in public debate.

---

66. Bruce Schneier, *Trusted Traveler Program*, CRYPTO-GRAM NEWSLETTER, Sept. 15, 2004, http://www.schneier.com/crypto-gram-0409.html#5.

67. *Commission Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC*, at 6, COM (2005) 438 final (Sept. 21, 2005), *available at* http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0438en01.pdf.

68. Prior to the data retention proposals, European privacy laws generally prohibited storage of communications records beyond the period needed for billing purposes. *See Directive 2002/58/EC of the European Parliament and of the Council*, 2002 O.J. (L 201) 37, 40 (EU), *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

69. A related risk came from the provision that gave access to the communications records to the police and, perhaps even worse, to terrorists and criminals who could get assistance from officials in any of the twenty-five E.U. Member States could get access to the records under accelerated procedures. *See Commission Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC*, *supra* note 67, at 6.

H. *What Are the Ramifications Internationally and with Other Stakeholders?*

The implicit focus thus far has been on the effects of an information sharing proposal on security for the United States. The next step in due diligence is to consider effects on other countries and on other possible stakeholders.

A prominent example since 9/11 has been the dispute between the U.S. and the European Union over U.S. access to passenger name records ("PNRs") for flights into and out of the United States.[70] The United States has sought electronic access to information about passengers including name, address, flight number, credit card number and so on. The European Union expressed concerns about how data would be handled about its citizens, and about compliance with E.U. privacy laws. In 2004, the United States issued a set of undertakings about how it will handle the data.[71] A key data protection committee in the E.U. has made a finding that the program is adequate under European law,[72] but legal challenges continue within Europe.[73]

Whatever the eventual outcome on PNRs, the dispute illustrates the importance of considering international ramifications of proposed information sharing programs. Among other possible issues, it is useful to consider four. First, the program may be lawful in the United States but violate the law in other countries. If so, then the program will likely be significantly more difficult to implement or may fail entirely. Second, international negotiations often take considerably longer to conclude than agreement within the U.S. government. Realistically, programs relying on international cooperation often demand a longer time frame. Third, U.S. agencies should be prepared for the possibility that other countries will expect information to be shared from the U.S. as well. It is prudent for the U.S. to consider whether it is willing to share its information with others, before expecting others to share with the United States. Fourth, U.S. proponents of an information sharing program should work cooperatively with the State Department and other entities that are knowledgeable

70. A detailed set of sources about the PNR debate is at http://www.epic.org/privacy/intl/passenger_data.html.

71. *See* Dep't of Homeland Sec., Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP) (May 11, 2004), http://www.dhs.gov/interweb/assetlibrary/CBP-DHS_PNRUndertakings5-25-04.pdf.

72. *See* Article 29 Data Protection Working Party, Opinion 8/2004 on the Information for Passengers Concerning the Transfer of PNR Data on Flights Between the European Union and the United States of America (Sept. 30, 2004), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp97_en.pdf.

73. In November, 2005, the Advocate General of the European Court of Justice advised that court to annul the PNR agreement on the grounds that the individual countries, rather than the E.U. itself, were the proper entities to negotiate such an agreement. *See* European Digital Rights, Advocate General European Court Rejects PNR Deal (Dec. 5, 2005), http://www.edri.org/edrigram/number3.24/PNR (linking to related documents).

about the diplomatic ramifications of a proposed program. An architecture that makes sense from a U.S. perspective may ruffle feathers overseas.[74]

Information sharing programs for U.S. national security are often conceived within a few agencies of the federal government. Increasingly, information sharing programs are contemplated internationally, or with states, localities and other organizations within the United States. Federal agencies have a limited ability to dictate to outside entities how information sharing should occur. Part of the due diligence for a new program, therefore, should be a thoughtful assessment of how these outside stakeholders may react. This assessment may lead to modification of how the information sharing program should proceed. In some instances, the legal and other concerns of outside entities will be severe enough that the program is not worth pursuing.

I. *Are There Privacy-Based Harms from the Proposed Measure?*

The next item in the due diligence list is an explicit examination of privacy-based harms that might result from a proposed measure. The discussion here first explains why the term "privacy" is not prominent earlier in the due diligence list, and then turns to the privacy-based harms.

1. *Why the Term "Privacy" Is Not Prominent in the Due Diligence List*

The discerning reader may have noticed an odd thing about the discussion thus far—in an article entitled *Privacy and Information Sharing in the War on Terrorism,* there have been only three passing references to privacy in the first eight items of the due diligence list.

In part, the lack of discussion of privacy is due to the vagueness of the term. The word privacy is used to cover a multitude of more specific concerns.[75] In creating a due diligence list, it thus works better analytically to refer to those concerns individually. For instance, it is a standard part of privacy discussions to refer to historical abuses and the need for checks and balances.

In greater measure, though, the downplaying of the term privacy reflects my pragmatic experience in assessing proposed information systems, both from outside government and from my time as Chief Counselor for

74. Another international area of dispute has flared up in British Columbia, where a major agency report has sought to prevent personal data of its citizens from being held in the United States and subjected to the USA-Patriot Act. *See* Information & Privacy Commissioner for British Columbia, Privacy and the USA-PATRIOT Act: Implications for British Columbia Public Sector Outsourcing (Oct. 2004), *available at* http://www.oipcbc.org/sector_public/usa_patriot_act/pdfs/report/privacy-final.pdf.

75. My views here are similar to those of Dan Solove, who uses Wittgenstein's idea of "family resemblance" to describe the multiple, related meanings of the word "privacy." *See* Daniel J. Solove, *Conceptualizing Privacy,* 90 CAL. L. REV. 1087, 1096-99 (2002) (describing that single word need not have any single meaning but can be used to represent several interconnected ideas).

Privacy during the Clinton administration. The due diligence list here reflects the questions I have found useful in working with those who propose or evaluate new information systems. Typically, some people in the process believe strongly in privacy, and are thus inclined to mold systems in privacy-protective ways. Others, however, have different views. The due diligence list shows the additional arguments that sometimes give such persons pause. Rigorous use of the due diligence list may create opportunities for fine-tuning a proposal or, occasionally, for making the decision that a program is not worth pursuing.

The due diligence list is designed to help decision makers avoid a rhetorical trap that often arises in privacy discussions. Discussions too often fall into the need to "balance" security and privacy, or find the right "trade-off" between the two. My experience is that constructive analysis typically ends the moment that talk turns to balancing or trade-off. After September 11 (and even before), the meeting ends this way: "You might make a good point, and I believe in privacy as much as the next person, but the current security challenges mean that we will all have to give up a little bit of our privacy." Put another way, security arguments seem tough and realistic, while privacy arguments seem soft and idealistic. When it comes to protecting the nation, tough and realistic will win pretty much every time.

Perhaps the reader, looking at this discussion, might decide that the entire due diligence list is just an effort at "spin," at finding palatable ways to sneak privacy concerns into security discussions. I offer a different perspective. The due diligence list is useful in practice because it focuses attention on the issues that are actually important and persuasive. If an information sharing proposal tips off our adversaries more than it helps us, then we should not do it. If a security proposal uses unprecedented measures that differ greatly from historical practice, there may be major unintended consequences, and those negative consequences should be avoided if possible. And so on for the other items on the due diligence list.

2. *Privacy-Based Harms*

To assist in due diligence on privacy-based harms, the discussion here looks at federal agency Privacy Impact Assessments (PIAs), a Department of Homeland Security Advisory Committee document that provides a framework for privacy analysis and some material from my own writings.

In 2000, the Federal Chief Information Officers Council adopted the idea of doing a PIA as a best practice for new federal agency IT systems.[76]

76. *See generally* FED. CHIEF INFO. OFFICER'S COUNCIL, BEST PRACTICES: PRIVACY; INTERNAL REVENUE SERVICE MODEL INFORMATION TECHNOLOGY PRIVACY IMPACT ASSESSMENT (2000), *available at* http://www.cio.gov/archive/pia_for_it_irs_model.pdf (adopting Privacy Impact Assessment of Internal Revenue Service as best practice to be adapted to other administrative agencies).

The E-Government Act of 2002 made a PIA a required step in the development or procuring of IT systems that include personally identifiable information.[77] Under the guidance for PIAs issued by the Office of Management and Budget, PIAs must analyze and describe:

1. what information is to be collected (e.g., nature and source);
2. why the information is being collected (e.g., to determine eligibility);
3. intended use of the information (e.g., to verify existing data);
4. with whom the information will be shared (e.g., another agency for a specified programmatic purpose);
5. what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent;
6. how the information will be secured (e.g., administrative and technological controls); and
7. whether a system of records is being created under the Privacy Act, 5 U.S.C. [§] 552a.[78]

In addition, the guidance is supposed to "ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information."[79] In essence, the PIA requires the agency to map the information flows of data into, through and out of a federal IT system and to determine the risk of harm from such data flows.

The Department of Homeland Security Data Privacy and Integrity Advisory Committee has recently adopted a thoughtful document entitled *Framework for Privacy Analysis of Programs, Technologies, and Applications* ("Framework").[80] The Framework overall takes an approach similar to the due diligence approach put forward in this Article. In its section of privacy and related interests, the Framework asks a series of structured questions. In summary, the questions address the following:

---

77. *See* E-Government Act of 2002 § 208, 44 U.S.C. Ch. 36.

78. Memorandum from Joshua B. Bolten, Dir. of the Office of Mgmt. and Budget, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, attachment A, pt. (II)(C)(1)(a) (Sept. 26, 2003), http://www.whitehouse.gov/omb/memoranda/m03-22.html (citation omitted).

79. *Id.* attachment B, pt. (B)(2)(b)(i).

80. *See* DATA PRIVACY AND INTEGRITY ADVISORY COMM., DEP'T OF HOMELAND SEC., REP. NO. 2006-1, FRAMEWORK FOR PRIVACY ANALYSIS OF PROGRAMS, TECHNOLOGIES, AND APPLICATIONS 1 (2006) *available at* http://www.privacilla.org/releases/DHS_Privacy_Framework.pdf (establishing framework within which to analyze security of technological applications and programs).

- *Confidentiality.* What rules and practices assure confidentiality of information?
- *Anonymity.* Is anonymity retained where that is reasonably possible?
- *Seclusion.* If the program fosters surveillance, are minimization practices in place, such as collection limitation, purpose specification, use limitation and retention limitation?
- *Fairness.* Are fairness and due process promoted, by compliance with criteria such as data quality, notice, individual participation and accountability, and transparency and accountability?
- *Liberty.* Does the program limit individual freedom, such as by conditioning freedom of movement or diminution of some privacy interest?
- *Data security.* How is personal information secured against threats to privacy and integrity?[81]

Along with these official documents, my earlier writings have attempted to analyze the sorts of harms that can result from surveillance. In *Financial Privacy and the Theory of High-Tech Government Surveillance,* I examined the sorts of harms that might occur if the government had routine access to every purchase made by individuals.[82] Types of harms notably include chilling effects (we might not act the same way if we are on camera), the burdens from complying with the surveillance (such as the time spent standing in long security lines in airports) and the privacy invasions themselves (ranging from identity theft to a non-tangible sense of invasion).[83] That article includes a detailed listing of possible privacy invasions.[84] One major but difficult to measure harm results from the privacy paradox: some surveillance measures are acceptable in the short term, but a long-term shift toward pervasive surveillance would be seen far more negatively.[85]

In short, by drawing on sources such as the E-Government Act of 2002, the Framework and scholarly writings, detailed due diligence is possible on the explicitly privacy-related harms that can arise from new information collection and sharing programs.

J. *Will Bad Publicity Undermine the Program?*

One last item for the due diligence list is to consider the possibility that the proposal will receive bad publicity once its existence becomes

81. *Id.* at 4-6.

82. *See generally* Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance,* 77 WASH. U. L.Q. 461 (1999) (describing disadvantages of government access to private information).

83. *See id.* at 472.

84. *See id.* at 493-507.

85. *See id.* at 461; Swire, *supra* note 19, at 1350.

known. There is an oft-repeated cycle where the government proposes a new program, privacy flaws are detected and immediate controversy swirls around the project. Among many examples might be numbered the cancellation or rollback of Total Information Awareness,[86] the CAPPS II passenger profiling program[87] and the Federal Intrusion Detection Network (FIDNet).[88] Indeed, during my time in government, one way I would get busy officials to focus on privacy issues was simply to give them recent press clips of government programs that had been canceled due to a privacy outcry in the press.[89]

It is useful to be specific about the way that bad publicity rationally fits within the due diligence process. First, sometimes bad publicity is an accurate reflection of problems with the proposed program—the program might look bad in the press because it is a bad idea, or because critics can accurately describe flaws. The task of preparing to discuss the program with the public may thus force proponents to confront a program's weaknesses.

Next, sometimes a program may seem worse in the press than it actually is. A complex program may be difficult to explain clearly, or sensationalistic anecdotes might be used by opponents. In addition, there may be a top secret basis for the program that cannot be disclosed. Even in such circumstances, I suggest, the possibility of negative press should be considered in advance. In a democracy, government programs will generally succeed over time only if they have public support. Considering how a program will look to the public thus is one step in the process of deciding whether and how to go forward with a program. In bureaucratic terms, it is often useful to vet a program with the press office and privacy experts before announcing the program. If those experts clear the program, it is

86. A detailed set of links about the Total Information Awareness program is available at Electronic Privacy Information Center, "Terrorism" Information Awareness (TIA), http://www.epic.org/privacy/profiling/tia (last visited May 10, 2006).

87. The original CAPPS II program was canceled and replaced with the less-ambitious Secure Flight program, which itself has received continuing criticism. A detailed set of links about the history is available at Electronic Privacy Information Center, Secure Flight, http://www.epic.org/privacy/airtravel/secureflight.html (last visited May 10, 2006).

88. *See* John Markoff, *U.S. Drawing Plan That Will Monitor Computer Systems*, N.Y. TIMES, July 28, 1999, at A1. By the next year, the front-page criticisms had turned into an uncontroversial program to purchase commercially-available software. *See* Christopher J. Dorobek, *GSA Kicks Off Effort for Intrusion Detection Service*, GOV'T COMPUTER NEWS, June 19, 2000, *available at* http://www.gcn.com/print/vol19_no16/2264-1.html.

89. For one discussion of the topic, focused on privacy press in the mid-1990s, see generally LAURA J. GURAK, PERSUASION AND PRIVACY IN CYBERSPACE: THE ONLINE PROTESTS OVER LOTUS MARKETPLACE AND THE CLIPPER CHIP (1997) (chronicling public debate about privacy issues, among others, surrounding launch of Lotus MarketPlace customer information software and government Clipper encryption technology during mid-1990s).

more likely to survive criticism from advocacy groups, the media, the Congress and the general public.

IV. CONCLUSION

The approach in this Article is intended to be practical—to gain the benefits from new information sharing programs while minimizing the risks to security, privacy and other goals. The due diligence checklist emerges from my own experience in creating and critiquing new information sharing programs. The checklist is designed to give constructive critiques of proposed programs before they are set in stone.

I hope that this sort of constructive critique becomes a regular part of the creation of new information sharing programs in the federal government. The due diligence list may prove useful to new institutional actors, such as the Chief Privacy Officers in federal agencies or the Privacy and Civil Liberties Board established by the 2004 intelligence reform law. Beyond this internal critique, the due diligence checklist can be used by Congress, the press and the general public to examine proposed programs and spot potential concerns. As we develop more information sharing programs, we can develop better methods for thoughtfully evaluating them.